REMARKS

In response to the Office Action mailed September 10, 2009, Applicant respectfully requests reconsideration. To further the prosecution of this Application, Applicant submits the following remarks. The claims as now presented are believed to be in allowable condition.

Claims 1, 2, 4-20, 31, 38-41 and 44-54 are pending in this Application. Claims 52-54 have been voluntarily amended to correct typographical errors and antecedent basis issues. The amendments do not add new matter to the Application and do not raise new issues requiring further searching and consideration. Claims 1, 38, and 47 are independent claims.

Preliminary Matters

In the present Application, a Petition to Accept an Unintentionally Delayed Priority Claim was submitted to the U.S. Patent Office on September 2, 2008. The Petition was dismissed on September 17, 2008. A Renewed Petition to Accept an Unintentionally Delayed Priority Claim, as well as an Amendment, was submitted to the U.S. Patent Office on November 18, 2008. The Decision on the Renewed Petition, issued on March 20, 2009, granted the present Application the benefit of the provisional Application No. 60/188,458, filed on March 10, 2000.

The Office Action, on page 2, indicates that Applicant's arguments filed on September 2, 1008 and November 18, 2008 have been considered. The Office Action further recites that "[t]his office action is based solely on the decision made 09/17/08. When a response to the petition filed on 11/19/08 is made, Examiner requests applicant to submit their response in accordance with the submitted petition decision."

Because the Renewed Petition granted the present Application the benefit of the provisional Application No. 60/188458, filed on March 10, 2000, Applicant

submits the following response in accordance with the Renewed Petition decision.

Rejections under §102

Claims 1, 2, 4-20, 31, 38-41 and 44-54 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,829,356 to Ford (hereinafter Ford).

Applicant respectfully traverses each of these rejections and requests reconsideration. The claims are in allowable condition.

The present Application was filed on March 9, 2001 and claims priority to a provisional application, serial number 60/188,458, filed on March 10, 2000. As indicated above, a Decision on the Renewed Petition, issued on March 20, 2009, granted the present Application the benefit of the provisional Application No. 60/188,458, filed on March 10, 2000.

It should be noted that provisional application serial number 60/188,458 provides support at least for independent claims 1, 38, and 47 recited in the present Application. Taking claim 1 as an example, claim 1 recites a method that includes implementing a multi-party secure computation protocol between a client which has a client secret and a server which has a server secret to compute a third secret from the client secret and the server secret, wherein the protocol is implemented so that the client obtains the third secret and cannot feasibly determine the server secret, and the server cannot feasibly determine the client secret and cannot feasibly determine the third secret. The method includes authenticating the client by a device, the device storing an encrypted secret and configured not to provide the encrypted secret without authentication and the device being distinct from the server and, after authenticating, providing to the client by the device the encrypted secret, wherein the encrypted secret is

capable of being decrypted using a decryption key derived from the third secret and wherein the multi-party secure computation protocol implemented between the client and the server is the only multi-party computation protocol that is implemented in generating the third secret and the decryption key derived from the third secret. Implementing the multi-party secure computation protocol involves, at the client, using the client secret to compute client information to harden the client secret and then sending the client information to the server, at the server, using the client information and the server secret to compute intermediate data and sending the intermediate data to the client and, at the client, deriving the third secret from the intermediate data. Support for at least independent claims 1, 38, and 47 is provided within provisional application 60/188,458, for example, on page 3, column 2 through page 4, column 1 (i.e., under the heading "5. A special case").

The Office Action has rejected independent claims 1, 38, and 47 under 35 U.S.C. §102(e) as being anticipated by Ford. Under 35 U.S.C. §102(e), a person shall be entitled to a patent unless:

> the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent…

Based upon the provisional application filing date for the present Application, Ford is not a proper reference under 35 U.S.C. §102(e) because embodiments of the invention described in the present Application were not described in "a patent granted on an application for patent by another filed in the United States *before the invention by the applicant* for patent."

Ford was filed on May 17, 2000 and clams priority to U.S. Provisional Patent Application Ser. No. 60/188,834, "Server-Assisted Regeneration of a

Strong Secret from a Weak Secret," by Warwick Ford, filed Mar. 10, 2000; U.S. Provisional Patent Application Ser. No. 60/167,453, "Secure Generation And Regeneration Of A Strong Secret From A Weak Secret Assisted By Multiple Servers," by Warwick Ford, filed Nov. 23, 1999; and U.S. Provisional Patent Application Ser. No. 60/141,571, "Password-Based Encryption And Recovery Protocol Immune To Password Guessing And Server Compromise," by Warwick Ford, filed Jun. 29, 1999.

As indicated above, the priority date for the present application is March 10, 2000. If the filing date of Ford (i.e., the utility application) of May 17, 2000 is taken as the 102(e) date, Ford is not a proper reference under 35 U.S.C. §102(e) because the priority date of the present Application (i.e., March 10, 2000) predates the filing date of Ford' s utility application. Accordingly, Ford does not constitute "a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent" as required by 35 U.S.C. §102(e).

Ford also claims priority to U.S. Provisional Patent Application Ser. No. 60/188,834 filed March 10, 2000. If the filling date of provisional application 60/188,834, March 10, 2000 is taken as the 102(e) date for Ford, Ford is not a proper reference under 35 U.S.C. §102(e) because the priority date of the present Application (i.e., March 10, 2000) falls on the same date as the filing date of Ford's provisional application. Accordingly, even with such a claim of priority, Ford does not constitute "a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent" as required by 35 U.S.C. §102(e).

Ford also claims priority to Provisional Patent Application Ser. No. 60/167,453, filed Nov. 23, 1999 and U.S. Provisional Patent Application Ser. No. 60/141,571, filed Jun. 29, 1999. While each one of these provisional patent

applications was filed before the priority date of the present application (i.e., before March 10, 2000) neither of Ford's provisional application describes embodiments of the invention presented in the present Application. Accordingly, if the filling date of either of these provisional application is taken as the 102(e) date, Ford is not a proper reference under 35 U.S.C. §102(e) because Ford is not "a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent" which describes embodiments of the invention presented in the present Application.

For the reasons stated above, because Ford does not constitute a proper reference under 35 U.S.C. §102(e), the rejection of claims 1, 38, and 47 under 35 U.S.C. §102(e) should be withdrawn. Accordingly, claims 1, 38, and 47 are in allowable condition. Because claims 2, 4-20, 31, 44-46, 49 and 52 depend from and further limit claim 1, claims 2, 4-20, 31, 44-46, 49 and 52 are in allowable condition for at least the same reasons. Because claims 39-41, 48, 50, and 53 depend from and further limit claim 38, claims 39-41, 48, 50, and 53 are in allowable condition for at least the same reasons. Because claims 51 and 54 depend from and further limit claim 47, claims 51 and 54 are in allowable condition for at least the same reasons.

Conclusion

In view of the foregoing remarks, this Application should be in condition for allowance. A Notice to this effect is respectfully requested. If the Examiner believes, after this Response, that the Application is not in condition for allowance, the Examiner is respectfully requested to call the Applicant's Representative at the number below.

Applicant hereby petitions for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this Response, including an extension fee, please charge any deficiency to Deposit Account No. 50-3661.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-2900, in Westborough, Massachusetts.

Respectfully submitted,

/Jeffrey J, Duquette/

Jeffrey J. Duquette, Esq.
Attorney for Applicant
Registration No.: 45,487
Bainwood, Huang & Associates, L.L.C.
Highpoint Center
2 Connector Road
Westborough, Massachusetts 01581
Telephone: (508) 616-2900
Facsimile: (508) 366-4688

Attorney Docket No.: 1048-006

Dated: October 26, 2009